Ročník 2010 electroscope Číslo II

Quantification of the safety level of a safety-critical control system

K. Rástočný [1], J. Ilavský[1]
[1] University of Žilina, Faculty of Electrical Engineering, Department of Control and Information Systems, Univezitná 8215/1, 010 26 Žilina, Slovak Republic
E-mail : karol.rastocny@fel.uniza.sk, juraj.ilavsky@fel.uniza.sk

Anotácia:
V článku je navrhnutá metóda výpočtu intenzity nebezpečných porúch bezpečnostne kritického riadiaceho systému priamo z rozdelenia pravdepodobnosti stavov absorpčného Markovovho reťazca so spojitým časom. Článok sa špecificky zameriava na absorpčné Markovove reťazce s viac než jedným absorpčným stavom. Navrhnutá metóda je na záver aplikovaná v konkrétnej prípadovej štúdii analýzy bezpečnostne kritického systému.

Annotation:
This paper introduces a method of evaluating the hazardous failure rate of a safety relevant control system if the state probability distribution is given as a result of an absorbing Continuous Time Markov Chain analysis. Markov Chains with more than one absorbing state are contemplated and eventually the case study is presented.

INTRODUCTION

Specific applications of control systems are closely related to a risk that outcomes of a control system failure could jeopardize the safety of a controlled process. A system is in those cases required to fulfil not only necessary control functions, but also safety or protective functions. Requirements on safety of a system are evaluated by means of a safety integrity level. Systems with those properties are referred to as safety related control system (SRCS).
The safety integrity level (SIL) has to be defined for every safety related function and it has to cover systematic failures as well as random failures [1].
The random failure integrity is in the case of electronic systems often achieved by massive redundancy application, which allows detection of a failure and negation of its consequences. Evaluation of the achieved SIL is based on quantitative methods. In general, random hardware failures mainly affect the technical safety of the system [1]
Required systematic failure integrity is usually reached by means of application of techniques used for systematic failures avoidance. Given serious problems when trying to assess reliability attributes of the systematic failures, it is virtually impossible to put quantitative methods into practice. Appraisal of the SIL is based on qualitative methods in this case. Systematic failures in the most cases affect the functional safety of the system [1].
There are four safety integrity levels specified (SIL1 to SIL4) in the standard [1] or in standards derived from it ([2] for instance). Numerically, those levels have meaning of tolerable hazard rate per safety related function. If an occurrence of a hazard is equated with an occurrence of a hazardous failure then hazardous failure rate per safety relevant function has to be determined instead.

SAFETY ASSESSMENT

The SRCS must be proved to fulfil all functional safety and technical safety requirements before being installed into an operation [3]. In another words, actual properties of the SRCS have to be compared with specification of safety requirements (Fig. 1).

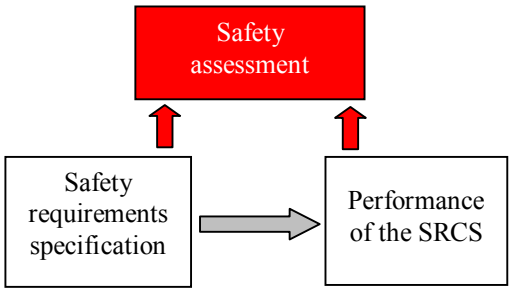

Fig. 1: Safety assessment principles

Functional safety requirements check can be done by the means of various test methods (e.g. module tests, integration tests, factory acceptance tests, site acceptance tests) and/or formal (semiformal) verification technique [5].
Technical safety requirements check cannot be based only on tests, but theoretical procedures and quantitative analysis methods have to be utilised instead [8]. Methods originally developed for the evaluation of dependability parameters can be successfully used to accomplish this goal (e.g. RBD, FTA, Markov Chains, Petri Nets).
Methods such as RBD and FTA are commonly used for the evaluation of safety parameters. The simplicity is their strong advantage; however in particular cases these methods suffer from inaccurate results. The use of these methods is limited to the analysis of items without possibility of recovery after a failure and with fundamental assumption that the

item can always be either in operational state or in complete non-operational state (or a safe state and a hazardous state when the safety is to be analysed). This assumption prevents us from considering more complexities affecting the safety of a system in the safety analysis (for instance failure rate, failure detection time, diagnostic coverage, reconfiguration of a system after a detection of a failure, system recovery etc.) [6].
More appropriate results of the safety analysis could be achieved by means of Markov Chains [7].

THEORETICAL BASIS

Random occurrence of the hardware failures can be considered to be a continuous stochastic process. In general, an analysed system can be in any state which belongs to a set S of states. If the change of the state is caused by an influence of any of the factors affecting the safety of the system and if Markovian property holds [3], then this system can be interpreted by the Continuous Time Markov Chain (CTMC).
The Markov analysis integrates qualitative as well as quantitative approach. The main task of the qualitative part of the analysis is to specify a state space of the analysed system. Number of states in the state space is a function of parameters considered in the analysis (e.g. faults, diagnostic properties and recovery), number of units in the system (the depth of decomposition) and also possibility of reconfiguration of the system after detection and negation of the failure. The goal of quantitative analysis is to evaluate what is the probability of the system being in the hazardous state. However, knowledge of the probability of the occurrence of hazardous state does not imply SIL of the system, since SIL is quantified through the hazardous failure rate of the system. When dealing with the CTMC with more than one absorbing state, evaluation of the hazardous failure rate of the system could be rather difficult.
The CTMC model which encompasses hardware failure outcomes and effects on safety of the SRCS has a default state - a failure-free state of the system. The CTMC has to contain at least one absorbing state which represents the hazardous state of the system. When there are more absorbing states present in the CTMC model, all of them could be eventually merged into two distinctive absorbing states (Fig. 2). Those are:

- hazardous state (referred to as H in Fig. 3 to 7);
- safe state (referred to as S in Fig. 3 to 7), which is reached after the detection and negation of the failure.

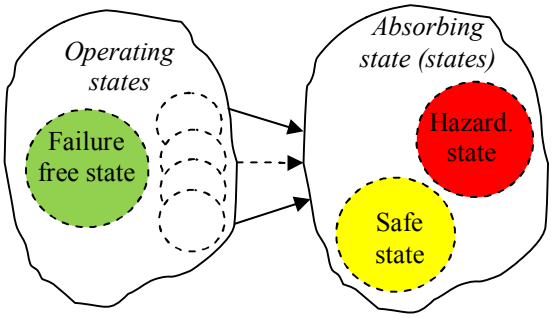

Fig. 2: General approach to the Markov modelling of a SRCS

There is an exact relation between the probability of the hazardous state and the hazardous failure rate which depends on particular probability distribution of a random variable. For continuous stochastic process we can state

$$\lambda(t) = \frac{\frac{dF(t)}{dt}}{1 - F(t)}, \tag{1}$$

where $\lambda(t)$ is a failure rate and $F(t)$ is a probability distribution function.
Every Markov Chain with only one absorbing state (Fig. 2) could be replaced by an equivalent diagram as pictured in Fig. 3.

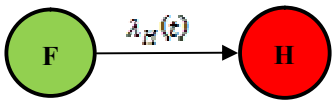

Fig. 3: Equivalent CTMC with one absorbing state

Diagram in Fig. 3 can be described by means of differential equations system (2) and its initial probability distribution $\mathbf{P}(t = 0) = \{1,0\}$.

$$\begin{aligned} \frac{dP_F(t)}{dt} &= -\lambda_H(t).P_F(t) \\ \frac{dP_H(t)}{dt} &= \lambda_H(t).P_F(t), \end{aligned} \tag{2}$$

where $\lambda_H(t)$ is a hazardous failure rate.
The probability of the system being in the H state has properties of the probability distribution function, therefore

$$\lambda_H(t) = \frac{\frac{dP_H(t)}{dt}}{1 - P_H(t)}. \tag{3}$$

The diagram (Fig. 2) with two absorbing states could also be replaced by an equivalent diagram. This case is represented by the diagram in Fig. 4.

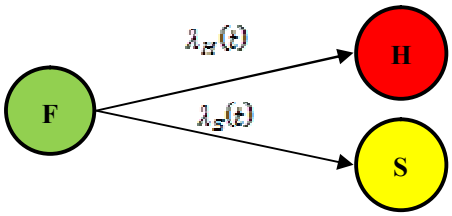

Fig. 4: Equivalent CTMC with two absorbing states

If $\lambda_S(t) \geq 0$ then $P_H(t)$ cannot be considered to be probability distribution function (for $t = \infty$ there is $P_H(t) < 1$, therefore (3) cannot be used to evaluate hazardous failure rate of the system.
Let us state:

$$P_{HS}(t) = P_H(t) + P_S(t), \quad \textbf{(4)}$$

$$\lambda_{HS}(t) = \lambda_H(t) + \lambda_S(t). \quad \textbf{(5)}$$

It is also valid that:

$$\frac{P_H(t)}{P_S(t)} = \frac{\lambda_H(t)}{\lambda_S(t)}. \quad \textbf{(6)}$$

Considering (3), (4), (5), (6) and the fact that the probability $P_{HS}(t)$ has properties of the probability distribution function, following statement holds:

$$\lambda_H(t) = \frac{\frac{dP_{HS}(t)}{dt}}{1 - P_{HS}(t)} \cdot \frac{P_H(t)}{P_{HS}(t)}. \quad \textbf{(7)}$$

CASE STUDY

Let us assume SRCS which is composed of two independent channels A and B which are identical in hardware architecture (Fig. 5) and they both control the controlled object CO. Channel A consists of sensor SA and unit UA; channel B consists of sensor SB and unit UB. The system would be in hazardous state only if both channels failed. Let us further assume that the failure rate of the random failures is constant and moreover $\lambda_A = \lambda_B = \lambda$ (which are actual assumptions when coping with a system composed of electronic elements).

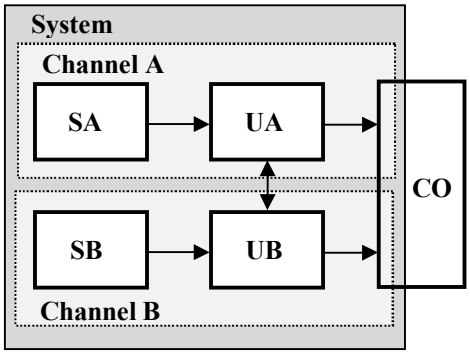

Fig. 5: The SRCS with 2-out-of-2 structure

If the system is not equipped with any failure detection mechanism then transition from the failure-free state F to the hazardous state H as a consequence of random failures can be modelled by diagram in Fig. 6. The system would be in the N state if only one channel has failed (either A or B).

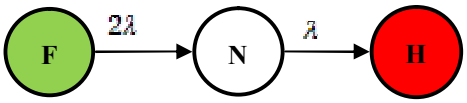

Fig. 6: The CTMC model of the system without the failure detection mechanism

The CTMC in Fig. 6 is mathematically described by the differential equations system (8) and initial probability distribution $\mathbf{P}(t = 0) = \{1,0,0\}$.

$$\frac{d\mathbf{P}(t)}{dt} = \mathbf{P}(t).\mathbf{A}, \quad \textbf{(8)}$$

where $\mathbf{P}(t = 0) = \{ P_F(t), P_N(t), P_H(t)\}$ is the time-dependent probability distribution and $\mathbf{A}$ is the infinitesimal generator matrix (9).

$$\mathbf{A} = \begin{pmatrix} -2\lambda & 2\lambda & 0 \\ 0 & -\lambda & \lambda \\ 0 & 0 & 0 \end{pmatrix}. \quad \textbf{(9)}$$

If we analytically solved (8) for $P_H(t)$, the result would be:

$$P_H(t) = \left(1 - e^{-\lambda.t}\right)^2. \quad \textbf{(10)}$$

Consequently derived transition rate from the failure-free state (the F state) to the hazardous state (the H state) would be:

$$\lambda_H(t) = \frac{2.\lambda.\left(1 - e^{-\lambda t}\right)}{\left(2 - e^{-\lambda t}\right)}. \quad \textbf{(11)}$$

However, if the system (Fig. 5) is equipped with failure detection and negation mechanism, then after the detection and negation of the failure it could reach the safe state (the S state in Fig. 7). This state could be abandoned only if the failure had been repaired and obligatory administrative measures had been carried out (this process has no primary impact on the SIL, therefore is not considered in Fig. 7). The failure detection is usually preformed by the means of data comparison of both units, so cross-communication between units is necessary. The CTMC model (Fig. 7) is constructed with the assumption that all potentially hazardous failures are covered by the failure detection mechanism.

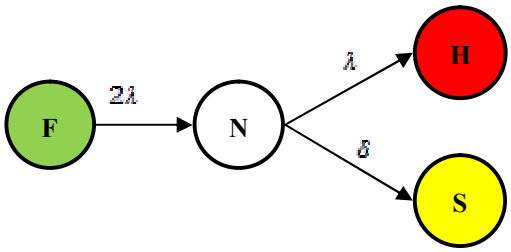

Fig. 7: The CTMC model of the system with the failure detection mechanism

The failure detection and negation rate can be determined from:

$$\delta = \frac{1}{t_D + t_N}, \tag{12}$$

where t_D is time to detection of the failure and t_N is time needed to negate its possible consequences [6].
Probabilities of the system being either in the H state or in the S state are given by (13) and (14) respectively.

$$P_H = \frac{\delta}{\lambda+\delta} + \frac{\delta}{\lambda-\delta}e^{-2\lambda t} - \frac{2\lambda^2}{\lambda^2-\delta^2}e^{-(\lambda+\delta)t} \tag{13}$$

$$P_S = \frac{\delta}{\lambda+\delta} + \frac{\delta}{\lambda-\delta}e^{-2\lambda t} - \frac{2\lambda\delta}{\lambda^2-\delta^2}e^{-(\lambda+\delta)t}. \tag{14}$$

Time-dependent probability of the hazardous state of the system (the H state) as a function of the failure detection and negation rate is shown in Fig. 7 (for $\lambda = 5.10^{-4}$ h^{-1}).

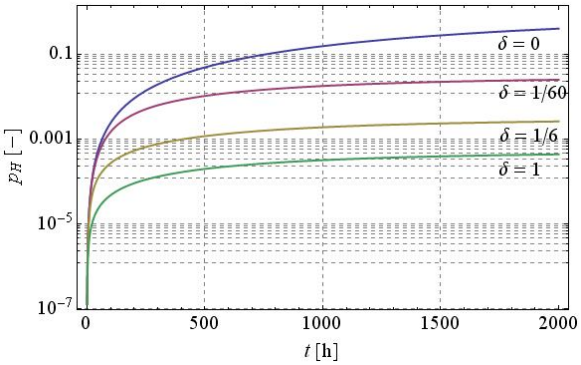

Fig. 8: Probability of the hazardous state of the system

Furthermore and with respect to (7), following equation can be derived (15).
The time-dependent hazardous failure rate as a function of various failure detection and negation rates δ is shown in Fig. 8 (assuming $\lambda = 5.10^{-4}$ h^{-1}).
The plots in Fig. 8 imply that 2-out-of-2 system with structure according to the Fig. 7, with failure rate $\lambda_A = \lambda_B = \lambda = 5.10^{-4}$ h^{-1} and time to detection and negation of the failure δ = 1 h, meets requirements that are laid down on SIL2 category system (when only random failures of a hardware are considered). In accord with the standard [1] or [2], value of the hazardous failure rate must be within the range specified (which is 1.10^{-6} h^{-1} to 1.10^{-7} h^{-1} for SIL2). Reduction of the hazardous failure rate in order to increase the SIL can be achieved by cutting down on a failure rate of the system or decreasing the time needed to detect and negate the failure.

$$\lambda_H = \frac{2\lambda\frac{(\lambda+\delta)}{(\lambda-\delta)}\left(e^{-(\lambda+\delta)t} - e^{-2\lambda t}\right)}{\left(\frac{2\lambda}{\lambda+\delta}e^{-(\lambda+\delta)t} - \frac{(\lambda+\delta)}{(\lambda-\delta)}e^{-2\lambda t}\right)} \cdot \frac{\left(\frac{\lambda}{\lambda+\delta} + \frac{\lambda}{\lambda-\delta}e^{-2\lambda t} - \frac{2\lambda^2}{\lambda^2-\delta^2}e^{-(\lambda+\delta)t}\right)}{\left(1 + \frac{\lambda+\delta}{\lambda-\delta}e^{-2\lambda t} - \frac{2\lambda}{\lambda-\delta}e^{-(\lambda+\delta)t}\right)} \tag{15}$$

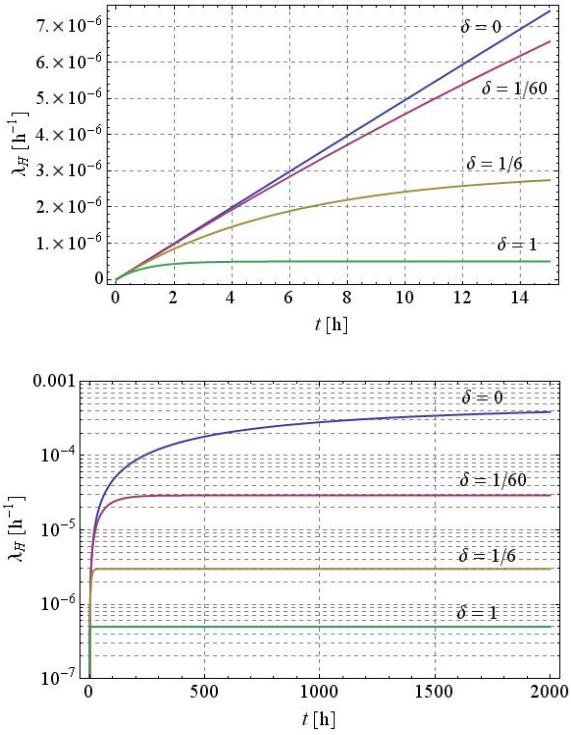

Fig. 9: Hazardous failure rate

CONCLUSION

The approach introduced in this paper was used for appraisal of random hardware failure modes effects on the safety integrity of electronic interlocking systems used in ŽSR operation. However, the systems in question are more complex than the case study above and embrace a wider range of levels of control.

ACKNOWLEDGMENT

This paper was supported by the scientific grant agency VEGA, grant No. VEGA-1/0040/08 "Mathematic-graphical modelling of safety attributes of safety-critical control systems".

REFERENCES

[1] EN IEC 61508: Functional safety of electrical/ electronic/programmable electronic safety-related systems. 2001.

[2] EN 50129: Railway application. Safety-related electronic systems for signalling. 2003.

[3] Börcsök, J.; Holub, P.; Schwarz, M. H.: How Safe is my System? Proceedings of the IEEE Conference ICONS'07, pages 40 – 45, ISBN 0-7695-2807-4.

[4] Brause, F.; Kritzinger, P.: Stochastic Petri Nets. page 49, Vieweg Verlag 2., 2002, ISBN 3-528-155535-3.

[5] Rástočný, K.; Janota, A.; Zahradník, J.: The Use of UML to Development of a Railway Interlocking System. In Journal: Lecture Notes in Computer Science, Springer-Verlag Heidelberg, 2004, pages 174-198, ISSN 0302-9743.

[6] Rástočný, K.: Primary Factors Affecting Safety of Control System. Modern Safety Technologies in Transportation MOSATT 2009. Proceedings of the International Sientific Conference. 22. – 24. september 2009, pages 225 – 230, ISBN 978-80-970202-0-0.

[7] Winkovich, T; Eckardt, D.: Reliability Analysis of Safety Systems Using Markov-Chain Modelling. Proceedings of the IEEE Conference EPE 2005, Dresden, pages P.1 – P10, ISBN 90-75815-08-50.

[8] Yu, J.; Johnson, B. W.: Safety Assessment for Safety-Critical Systems Including Physical Faults and Design Faults. Reliability and Maintainability Symposium RAMS '06, 2006, pages 588 – 593, ISSN 0149-144X.